UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/521,741	01/18/2005	Craig B. Gentry	M-16094 US	7038

32605 7590 06/10/2009

Haynes and Boone, LLP
IP Section
2323 Victory Avenue
SUITE 700
Dallas, TX 75219

EXAMINER	
ARMOUCHE, HADI S	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
06/10/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/521,741	GENTRY, CRAIG B.	
	Examiner	Art Unit	
	HADI ARMOUCHE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26,117,118,120,124-139,141-143,145 and 149-239* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26, 117-118, 120, 124-139, 141-143, 145 and 149-239* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 March 2009* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to applicant's amendment filed on 03/04/2009. Claims 1, 8, 9, 13-15, 17-18, 24, 26, 117, 118, 120, 124-136, 138-139, 141-143, 145 and 149-183 have been amended, claims 174-239 have been added, claims 27-116, 119, 121-123, 140, 144 and 146-148 have been cancelled. Claims 1-26, 117-118, 120, 124-139, 141-143, 145 and 149-239 remain pending.

2. Acknowledgement to applicant's amendment to the specification has been noted. The amendment has been reviewed and entered and found obviated to previously raised objection for minor informalities. Objection to the specification is hereby withdrawn.

3. Acknowledgement to applicant's amendment to the abstract has been noted. The amendment has been reviewed and entered and found obviated to previously raised objection for using legal phraseology. Objection to the abstract is hereby withdrawn.

4. Acknowledgement to applicant's amendment to the drawing has been noted. The amendment has been reviewed and entered and found obviated to previously raised objection for minor informalities. Objection to the drawings is hereby withdrawn.

5. Applicant's amendment to claims 126 and 127 obviate previously raised claim objection for mis-numbering the claims in the application. Claim objection to claims 126 and 127 is hereby withdrawn.

6. As discussed in an interview on 02/27/2009, the examiner interprets the manufacture of claims 156-183 to be a memory as supported in paragraph 192 of the

specification. Hence, the rejection of claims 156-183 under 35 USC 112, first and second paragraphs is hereby withdrawn.

7. Applicant's amendment to claims 1 and 18 obviate previously raised rejection of claims 1-26 and 117-183 under 35 USC 112, second paragraph. Rejection of claims 1-26 and 117-183 under 35 USC 112, second paragraph is hereby withdrawn.

8. Applicant's amendment to claims 1, 18 and 156-183 obviate previously raised rejection of claims 1-26 and 117-183 under 35 USC 101. Rejection of claims 1-26 and 117-183 under 35 USC 101 is hereby withdrawn.

Election/Restrictions

9. Claims 27-116 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected inventions, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 09/15/2009.

Response to Arguments

10. Applicant's arguments (page 38 of the remarks) with respect to the newly amended limitations of claims 1 and 18 have been considered but they are not persuasive. The amendment was extensive and the citations in the grounds of rejection with respect to the amended language and the Boneh reference are set at below.

Claim Objections

11. Claims 172, 173, 177 and 181 are objected to because they depend on cancelled claims. For the purpose of examination, examiner assumed that claims 172, 173, 177 and 181 depend on claims 120, 124, 139 and 149 respectively.

12. Claim 137 is objected to for it refers to operation S of claim 15. "Operation S" has been removed from claims 1 and 15. Appropriate correction is required.

13. Applicant is advised that should claim 1 be found allowable, claim 184 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15. Claims 1 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Boneh et al. (US 7,113,594, cited on IDS dated 9/3/2008) referred to hereinafter by Boneh.

16. Regarding claims 1, 18, 184, 218 and 229, Boneh teaches *a method for operating a public-key encryption scheme which provides for sending a digital message M between a sender and a recipient with participation of an authorizer, wherein the digital message is encrypted by the sender and decrypted by the recipient, the method*

comprising encrypting, by at least one machine in a set of one or more machines, the digital message M using at least a recipient public key and a recipient encryption key to create an encrypted digital message for decryption with a recipient private key and a recipient decryption key, wherein: the recipient public key and the recipient private key form a public key/ private key pair, wherein the recipient private key is a secret of the recipient; the recipient decryption key is generated using at least a key generation secret of the authorizer and the recipient encryption key, wherein a key formed from the recipient encryption key and a key formed from the recipient decryption key are a public key/ private key pair [abstract, col 3 lines 4-12, col 4 lines 1-15, col 9 line 49-col 10 line 4, col 15 lines 1-67 and col 24 lines 29-67].

17. Regarding claims 2, 19, 185, 204, 219 and 230, Boneh teaches that *the recipient encryption key is generated from information comprising the identity of the recipient* [col 2 lines 48-55].

18. Regarding claims 3, 20, 186, 205, 220 and 23, Boneh teaches that *the recipient encryption key is generated from information comprising a parameter defining a validity period for the recipient decryption key* [col 2 lines 48-55].

19. Regarding claims 4, 21, 187, 206, 221 and 232, Boneh teaches that *the recipient encryption key is generated from information comprising the recipient public key* [col 2 lines 62-65].

20. Regarding claims 5, 22, 188, 207, 222 and 233, Boneh teaches that *the recipient encryption key is generated from information comprising the identity of the recipient, the*

recipient public key, and a parameter defining a validity period for the recipient decryption key [col 2 lines 48-62].

21. Regarding claims 6, 23, 137, 189, 208, 223 and 234, Boneh teaches that *the recipient decryption key is generated by the authorizer according to a schedule known to the sender* [col 2 lines 48-62 and col 16 lines 1-19].

22. Regarding claims 7, 190 and 209, Boneh teaches that *the recipient encryption key is generated using at least information comprising the schedule* [col 2 lines 48-62 and col 16 lines 1-19].

23. Regarding claims 8, 24, 191, 224 and 235, Boneh teaches that *the recipient private key and the recipient public key are generated using at least one system parameter issued by the authorizer* [col 2 lines 48-62 and col 16 lines 1-19].

24. Regarding claims 9, 192 and 210, Boneh teaches that *wherein the recipient decryption key is generated by the authorizer to have a value $S = s_c P_B$, wherein: s_c is the key generation secret of the authorizer; and P_B is the recipient encryption key and is equal to $H_1(Inf_B)$, wherein Inf_B is an element of a first cyclic group $\mathbb{G}_1$ of elements, wherein P_B is an element of ~~and~~ a second cyclic group $\mathbb{G}_2$ of elements, and H_1 is a predefined function ("first function H_1"), wherein the first and second cyclic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ and the function H_1 are system parameters made available to the sender, and also available to the sender are system parameters comprising: a generator P of the first cyclic group $\mathbb{G}_1$; a key generation parameter $Q = s_C P$; a second function H_2 capable of generating a second string of binary digits from an element of the second*

cyclic group $\mathbb{G}_2$ [col 3 lines 32-55, col 5 line 52-col 6 line 44, col 7 line 6-15, col 7 line 30-37, col 14 and col 15].

25. Regarding claims 10, 193 and 211, Boneh teaches that *Inf_B comprises the identity of the recipient, ID_{rec}, the recipient public key, and a parameter defining a validity period for the recipient decryption key* [col 2 lines 48-62 and col 16 lines 1-19].

26. Regarding claims 11, 194 and 212, Boneh teaches that *both the first group* $\mathbb{G}_1$ *and the second group* $\mathbb{G}_2$ *are of the same prime order q* [col 6 lines 15-23].

27. Regarding claims 12, 195 and 213, Boneh teaches that *the first cyclic group* $\mathbb{G}_1$ *is an additive group of points on a super singular elliptic curve or abelian variety, and the second cyclic group* $\mathbb{G}_2$ *is a multiplicative subgroup of a finite field* [col 24 lines 5-27].

28. Regarding claims 13, 196 and 214, Boneh teaches that *the system parameters available to the sender further comprise a function ê which is a bilinear, non-degenerate, and efficiently computable pairing which maps* $\mathbb{G}_1 X \mathbb{G}_1$ *into* $\mathbb{G}_2$ [col 24 lines 5-27].

29. Regarding claims 14, 197 and 215, Boneh teaches that *s_C is an element of the cyclic group* $\mathbb{Z}/q\mathbb{Z}$ [col 24 lines 5-27].

30. Regarding claims 15 and 198, Boneh teaches *encrypting the digital message M comprises: generating an element $P'_B = H_1(ID_{rec})$, wherein ID_{rec} comprises the identity of the recipient and wherein H_1 is a function capable of generating an element of the*

first cyclic group $\mathbb{G}_1$ from a string of binary digits;selecting a random key generation secret r; and encrypting the digital message M to form a ciphertext C, wherein C is set to be: C = [rP, M $\oplus H_2(g^r)$], where g = $\hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, where PK_B is the recipient public key and wherein $\hat{e}$ is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 X \mathbb{G}_1$ into $\mathbb{G}_2$ [col 5 lines 40-col 6 line 65].

31. Regarding claims 16, 199 and 216, Boneh teaches that *the recipient encryption key is generated from a document and the recipient decryption key is the authorizer's signature on the document* [abstract].

32. Regarding claims 17 and 200, Boneh teaches that *encrypting the digital message M comprises: generating an element $P'_B = H_1(ID_{rec})$ wherein H_1 is a function capable of generating an element of the first cyclic group $\mathbb{G}_1$ from a string of binary digits; choosing a random parameter $\sigma \in \{0,1\}^n$; set a random key generation secret $r = H_3(\sigma, M)$; and encrypting the digital message M to form a ciphertext C, wherein C is set to be: C = [rP, M $\oplus H_2(g^r)$, $E_{H_4(\sigma)}(M)$], where g = $\hat{e}(Q, P_B)\hat{e}(PK_B, P'_B) \in \mathbb{G}_2$, wherein PK_B is the recipient public key, wherein H_3 is a function capable of generating an integer of the cyclic group $\mathbb{Z}/q\mathbb{Z}$ from two strings of binary digits, H_4 is a function capable of generating one binary string from another binary string, E is a symmetric encryption scheme, $\hat{e}$ is a bilinear non-degenerate pairing which maps $\mathbb{G}_1 X \mathbb{G}_1$ into $\mathbb{G}_2$, and $H_4(\sigma)$ is the key used with E* [col 5 lines 40-col 6 line 65 and col 24 lines 5-27].

33. Regarding claims 25, 142, 225 and 236, Boneh teaches that *the recipient decryption key is related to the root key generation secret and the associated root key generation parameter* [col 25 lines 38-50].

34. Regarding claims 26, 226 and 237, Boneh teaches that *the plurality of authorizers further includes at least m lower-level authorizers in the hierarchy between the root authorizer and the sender, wherein m ≥ 1, and wherein I of the m authorizers in the hierarchy are common ancestors to both the sender and the recipient, wherein authorizer is the lowest common ancestor authorizer between the sender and the recipient, and wherein I ≥ 1, and wherein a lower-level key generation secret is selected for each of the m lower-level authorizers in the hierarchy between the root authorizer and the sender; and a sender decryption key is generated such that the sender decryption key is related to at least the root key generation secret and one or more of the m lower-level key generation secrets associated with the m lower-level authorizers in the hierarchy between the root authorizer and the sender; wherein the message is encrypted using at least the sender decryption key and one or more of the lower-level key generation parameters associated with the (m – I +1) authorizers between the root authorizer and the sender that are at or below the level of the lowest common ancestor authorizer, but not using any of the lower-level key generation parameters that are associated with the (I - 1) authorizers above the lowest common ancestor authorizer; and wherein the encrypted digital message is decryptable using at least the recipient decryption key and one or more of the lower-level key generation parameters associated with the (n – I + 1) authorizers between the root authorizer and the sender*

that are at or below the level of the lowest common ancestor authorizer$_i$, but not using any of the lower-level key generation parameters that are associated with the (I - 1) authorizers that above the lowest common ancestor authorizer$_i$. [col 15 lines 45-53, col 24 lines 53-54 and col 25 lines 38-64].

35. Regarding claims 117, 120, 139, 141 and 145, Boneh teaches that *the method further comprises the recipient performing, by at least one machine in the set of the one or more machines, operations of: generating the recipient public key and the recipient private key; decrypting the encrypted digital message using at least the recipient private key and the recipient decryption key* [abstract, col 3 lines 4-12, col 4 lines 1-15, col 9 line 49-col 10 line 4, col 15 lines 1-67 and col 24 lines 29-67].

36. Regarding claims 118 and 201, Boneh teaches that *the method further comprises the authorizer selecting, by at least one machine in the set of the one or more machines, said key generation secret and generating the recipient decryption key and sending the recipient decryption key to the recipient* [abstract, col 3 lines 4-12, col 4 lines 1-15, col 9 line 49-col 10 line 4, col 15 lines 1-67 and col 24 lines 29-67].

37. Regarding claims 124-128, 130 and 149-151, Boneh teaches *generating, by at least one machine in the set of the one or more machines, the recipient encryption key by the authorizer and/or the recipient and/or the sender* [abstract, col 3 lines 4-12, col 4 lines 1-15, col 9 line 49-col 10 line 4, col 15 lines 1-67 and col 24 lines 29-67].

38. Regarding claims 129, 131-136 and 138, Boneh teaches that *the method further comprises the authorizer selecting, by at least one machine in the set of the one or*

more machines, said key generation secret and generating, by at least one machine in the set of the one or more machines, the recipient decryption key and sending, by at least one machine in the set of the one or more machines, the recipient decryption key to the recipient [abstract, col 3 lines 4-12, col 4 lines 1-15, col 9 line 49-col 10 line 4, col 15 lines 1-67 and col 24 lines 29-67].

39. Regarding claim 137, Boneh teaches that *the method comprises the operation (S) performed by the sender* [abstract and col 15 lines 1-67].

40. Regarding claims 143,154-155, 227 and 238, Boneh teaches that *the method further comprises generating, by at least one machine in the set of the one or more machines, the recipient decryption key by one of the authorizers* [abstract, col 3 lines 4-12, col 4 lines 1-15, col 9 line 49-col 10 line 4, col 15 lines 1-67 and col 24 lines 29-67].

41. Regarding claims 156-183, 202, 217, 228 and 239, Boneh teaches *a computer-readable manufacture comprising a computer-readable computer program operable to cause a computer to perform the method of claim 1* [col 26 lines 3-13].

Conclusion

42. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432